



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

HW

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/937,883	09/25/1997	SHIMON GRUPER	COLB-0083	2262
20741	7590	05/19/2005	EXAMINER	
HOFFMAN WASSON & GITLER, P.C			TANG, KENNETH	
CRYSTAL CENTER 2, SUITE 522			ART UNIT	PAPER NUMBER
2461 SOUTH CLARK STREET				2195
ARLINGTON, VA 22202-3843				

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	08/937,883	GRUPER ET AL.
	Examiner Kenneth Tang	Art Unit 2195

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 07 April 2005.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 19 and 21-44 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 19 and 21-44 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

DETAILED ACTION

1. This action is in response to the Amendment on 4/4/05. Applicant's arguments have been fully considered but were not found to be persuasive. In addition, new grounds of rejections were made on newly added claims 40-44.
2. Claims 19 and 21-44 are pending in the application.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 19 and 21-44 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Learning only the normal behavior of the application is the subject matter that was not described in the specification (claim 36). Applicant has pointed to page 9, lines 11-17 of their specification. However, this section as well as the entire specification fails to provide the written description for learning only the normal behavior of the application. At best, the specification discloses attempting to learn when falling within certain parameters. However, this does not indicate normal behavior and the specification does not define the normal behavior to have any structural relationship with any certain parameters. In fact, it is not even disclosed in the specification the definition of what a relative term like normal is (to support of claims 19, 22,

24, and 25). There is no distinct connection that defines “normal” to be related to “permitted” activities over “forbidden” activities on page 9, lines 11-17 of the specification.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 41-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention:

- a. In claim 41, there is no relationship made between the “abnormal behavior” (in the preamble) to anything else in the body of the claim.
- b. In claims 42, there is no relationship established or made between “normal access behavior” (in the preamble) with anything else in the body of the claim.

Claim Rejections - 35 USC § 101

5. The program that performs the method of newly added claims 42-44 are non-statutory as not being tangibly embodied in a manner so as to be executable. This is true even if the method of claims 42-44 are a statutory method.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 19, 21-39, and 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shieh et al. (hereinafter Shieh) (US 5,278,901) in view of Crosbie et al. (hereinafter Crosbie) “Active Defense of a Computer System using Autonomous Agents”.

7. As to claim 19, Shieh teaches an apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise comprising:

- an enforcement device, operative after said period is over, for identifying said application from accessing elements of data storage that do not correspond with the normal behavior of said application (*“pattern-oriented instruction detection system and method that defines patterns of intrusion”*, see *Abstract*, *“intrusion detection system”*, see *Fig. 2, item 215, col. 9, lines 5-6 and 67, “present protection graph 205”*, *col. 9, line 65, col. 18, lines 50-56, col. 1, lines 17-19*);

Shieh fails to explicitly teach:

- apparatus for learning about the normal behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to elements of said data storage during a limited period and preventing access;

8. However, Crosbie teaches an intruder detection system that recognizes the intruder, learns about the intrusions, and prevents (disallows) possibly intruders (*“Intruder recognition”*, *“Learning about intrusions”*, *“Response to an intrusion”*, *page 4, right hand column, page 2, 1st*

column, last paragraph through 2nd column, first paragraph, and lines 36-39, page 6, left hand col. Lines 33-36, right hand col. Lines 8-10).

9. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Shieh and Crosbie because Crosbie's feature of learning about the normal behavior of said application by monitoring accesses of said application to elements of said data storage would improve the accuracy of dealing with the intrusion. The knowledge learned about intrusions is used in future decisions of responding to an intrusion ("learn about intrusions and use that knowledge in future decisions", page 4, col. 2, 2nd bullet point).

10. As to claim 21, Crosbie teaches an apparatus wherein said enforcement device is operative to prompt a user to give specific permission, upon occurrence of an attempt of the program to access files not accessed during said learning period. Crosbie teaches a system which recognizes intrusions, learns about the intrusions, and responds/deals with the intrusions that are detected and are based by a human operator ("anomalous activity", "human operator", page 6, col. 2, "Intruder recognition", "Learning about intrusions", "Response to an intrusion", page 4, col. 2, "observe deviations from normal behaviour", page 5, col. 1, "Cooperative monitoring", see Abstract). Shieh in view of Crosbie fails to explicitly teach that the verification data for each program is stored in a file and that file is accessed for verification. However, "Official Notice" is taken that both the concept and advantages of providing that data can be stored in a file is well known and expected in the art. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a file that contained the

verification data of each program to the existing system for the reason of increasing organization of the program by keeping the verification information for a particular program in one area. It makes it simpler for the respective program to access the information.

11. As to claim 23, it is rejected for the same reasons as stated in the rejection of claim 21. Furthermore, it is obvious that there is more leniency to access files with user permission because there is no leniency without permission.

12. As to claims 22 and 24, Shieh teaches an apparatus for ensuring the integrity of a computer application to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising:

- apparatus for assigning a general enforcement file to each new program (*“protection sets help define the targets of intrusion detection”*, col. 8, lines 19-20, *“audit trails”*, *“protection graph”*, col. 8, lines 37-49);

Shieh fails to explicitly teach:

- apparatus for learning about the program by monitoring the program of said data storage, by monitoring the program's attempts to make file accesses during a learning period;
- an enforcement device operative, after said learning period is over, to treat attempts of the program to access files accessed during said learning period more leniently than attempts of the program to access files not accessed during said learning period, said enforcement device is based at least on instances of specific permission being given by the user to said application to access locations of said data storage, wherein said enforcement device

treats attempts of said application to access locations of said data storage to which the user has permitted to access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period.

13. However, Crosbie teaches a system which recognizes intrusions, learns about the intrusions, and responds/deals with the intrusions that are detected and are based by a human operator ("anomalous activity", "human operator", page 6, col. 2, "Intruder recognition", "Learning about intrusions", "Response to an intrusion", page 4, col. 2, "observe deviations from normal behaviour", page 5, col. 1, "Cooperative monitoring", see Abstract). Shieh fails to explicitly teach that the verification data for each program is stored in a file. However, "Official Notice" is taken that both the concept and advantages of providing that data can be stored in a file is well known and expected in the art. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a file that contained the verification data of each program to the existing system for the reason of increasing organization of the program by keeping the verification information for a particular program in one area. It makes it simpler for the respective program to access the information.

14. As to claim 25, it is rejected for the same reasons as stated in the rejection of claim 24.

15. As to claim 26-28, Crosbie teaches a method further comprising enabling the user of said first application to determine said normal behavior during said learning period (see rejection of claims 24 and 25).

16. As to claim 29-34, Shieh in view of Crosbie teaches a method further comprising detecting attempts of a daughter or second application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon. It is rejected for the same reasons as stated in the rejection of claims 22 and 24. In addition, Shieh teaches detection on two applications (*“detection of unintended use of foreign programs and detection of virus propagation”*, col. 4, lines 10-23).

17. As to claim 35, it is obvious to have a second application is executed on a second computer for the reason of increasing the speed of running the application by not using the resources of the first computer to run the second application.

18. As to claims 36-39, Sheih teaches the learning with respects to claim 19 learns only the normal behavior of the application (*col. 2, lines 34-41, col. 8, lines 19-20*). Items stored in the protection graph is only of the normal behavior. Once the normal items in the protection graph are learned, it is then compared to the items in the set of intrusion patterns.

19. As to claim 42, it is rejected for the same reasons as stated in the rejection of claim 19. In addition Shieh teaches having a list of access permissions (“privileges”) (*see Abstract, col. 4, lines 30-49, e.g.*).

20. As to claim 43, it is inherent that during a limited period in which said program is assumed to be uninfected by a virus, upon indicating by said monitoring a request to access an element of data storage which is not on said list, adding said element to said list as allowable for access because if an allowed program is not added to the list as allowable (rather than not allowable or given that specific privilege/permission), the system would not work correctly.

21. As to claim 44, Shieh teaches wherein said monitoring further includes requests of a daughter application of said program to access data storage (accessing foreign program that does not contain a virus, e.g.) (*col. 4, lines 63-66*).

22. **Claims 40-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shieh et al. (hereinafter Shieh) (US 5,278,901) in view of Crosbie et al. (hereinafter Crosbie) “Active Defense of a Computer System using Autonomous Agents”, and in further view of Hayman et al. (hereinafter Hayman) (US 5,859,966).**

23. As to claim 40, it is rejected for similar reasons as stated in the rejection of claim 19. However, Shieh and Crosbie fail to explicitly teach granting the application no access rights to any elements of data storage other than those elements accessed during the limited period, to which access will be allowed. Hayman teaches a virus program prevention security system with various privileges in that it when a process such as monitoring or diagnosing period is completed, granting said application no access rights to any elements of data storage oether than

those elements accessed during said limited period, to which access will be allowed (*see Abstract, col. 7, lines 57-60 and col. 8, lines 60-62, e.g.*). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the references of Hayman with Shieh and Crosbie because the containment and privileges would increase the security of the existing system (*col. 1, lines 48-67*).

24. As to claim 41, it is rejected for similar reasons as stated in the rejection of claim 25. However, Shieh and Crosbie fail to explicitly teach granting the application no access rights to any elements of data storage other than those elements accessed during the limited period, to which access will be allowed. Hayman teaches a virus program prevention security system with various privileges in that it when a process such as monitoring or diagnosing period is completed, granting said application no access rights to any elements of data storage other than those elements accessed during said limited period, to which access will be allowed (*see Abstract, col. 7, lines 57-60 and col. 8, lines 60-62, e.g.*). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the references of Hayman with Shieh and Crosbie because the containment and privileges would increase the security of the existing system (*col. 1, lines 48-67*).

Response to Arguments

25. *Applicant argues on the first page of the Remarks that claims 36-39 does comply with the written description requirement of 35 USC 112, 1st paragraph. Applicant points to page 6, second paragraph, taken in conjunction with page 9, lines 11-17.*

In response, the Examiner respectfully disagrees. The Applicant relates the definition of “normal” (normally) to be associated with permitted activities. However, there is no connection whatsoever in the specification of this association. For the same reasons, one could equally associate normal to be “forbidden”. The specification does not make it explicitly clear whether normal relates to “permitted” or “forbidden”.

26. *Applicant demonstrates (on page 2 of the Remarks) that the learning mode as being taught in the specification and complying with the 35 USC 112, 1st paragraph.*

In response, the Examiner does not question the written description compliance of this. The Examiner is concerned with the lack of support in the specification of the definition of “normal” as being explicitly defined to relate to “permitted” activities and not “forbidden” ones.

27. *Applicant argues on pages 2-3 of the Remarks that Shieh nor Crosbie teaches the actual prevention or restriction of the detected abnormal behavior but instead detects the intrusion after the fact.*

In response, the Examiner respectfully disagrees. Crosbie teaches preventing (“disallowing”) the detected abnormal behavior (*page 2, 1st column, last paragraph through 2nd column, 1st paragraph*).

28. *Applicant’s newly added claims have prompted the new grounds of rejections.*

29. *Applicant points out (on the last page of the Remarks) that the Applicant’s invention prevents access from a program, whereas the prior art focuses on the user.*

In response, Shieh teaches intrusions to be foreign programs containing viruses and Trojan horses (*col. 2, lines 18-22*). Therefore, Applicant's argument is not found to be persuasive.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kenneth Tang whose telephone number is (571) 272-3772. The examiner can normally be reached on 8:30AM - 6:00PM, Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kt
5/16/05


MENG-AL T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100